

Ontrack® Data Recovery



Whitepaper Datenrettung

KROLL ONTRACK®

Vertrauen Sie auf die Besten.

Inhaltsverzeichnis

Whitepaper: Datenrettung	2
Was sind Daten eigentlich wert?	3
Folgen von Datenverlust	4
Wie kommt es zu Datenverlust?	5
Gefährdete Speichermedien	7
Magnetisch und optisch gespeicherte Daten auf stationären Systemen	7
Mobile Daten	9
Speichermethoden	10
Methoden der Datenrettung	11
Wiederherstellung der Daten	11
Datenrettung im Labor / Reinraum	12
Online-Datenrettung	13
Datenrettung mit Software-Tools	16

Whitepaper: Datenrettung

Sofortmaßnahmen bei Datenverlust

Sobald Sie einen Datenverlust festgestellt haben:

1. Schalten Sie das betroffene Gerät aus!
2. Lassen Sie das System ausgeschaltet. Ein Neustart kann hier zu einer Verschlimmerung führen!
3. Die Installation neuer Software kann Schäden vergrößern.
4. Sorgen Sie dafür, dass das Rechnergehäuse und natürlich die Festplatte ungeöffnet bleiben.
5. Wenden Sie sich unbedingt an ein Fachunternehmen für Datenrettung, wie z.B.:

Notfall (kostenlos): 0800 10 12 13 14 (D)
 0800 644 150 (A)
 0800 880 100 (CH)

E-Mail: info@krollontrack.de
 info@krollontrack.at
 info@krollontrack.ch

Internet: www.ontrack.de | www.krollontrack.de
 www.ontrack.at | www.krollontrack.at
 www.datenrettung.ch | www.recuperationdedonnees.ch | www.krollontrack.ch

6. Geben Sie folgende Informationen an:

- eingesetztes Betriebssystem
- Art, Hersteller und Modell des betroffenen Speichermediums
- Speicherkapazität des Mediums
- Art des Problems, Symptome, Umstände des Datenverlustes
- Ob ein Virens Scanner eingesetzt wurde
- Ob Sie in letzter Zeit ein Virenproblem hatten
- Ob Sie bereits selbst versucht haben, mit einem Tool die Daten zu retten

Was sind Daten eigentlich wert?

Buchhaltung, Kalkulation, Kundenverwaltung, interne und externe Kommunikation, Ideen, Konzepte, Patente – Fundament, Wissen und Visionen eines Unternehmens finden sich heute in Firmencomputern. Dabei überschreitet der Informationsgehalt der gespeicherten Daten bei weitem das Potenzial, das einst in Aktenschränken gelagert wurde. Hierzu tragen nicht zuletzt die beliebige Verknüpfbarkeit verschiedener Prozesse, der universelle Zugriff und die ständige Verfügbarkeit des gesamten Wissensschatzes bei.

Tatsächlich ist sich aber kaum ein Unternehmen des Wertes seiner Daten bewusst. Mittlerweile kann zwar nicht mehr nur die Hardware versichert werden, sondern auch der Datenbestand, die Wertbestimmung von Daten ist jedoch recht beliebig. Ob der Versicherungsschutz tatsächlich die Kosten abdeckt, die bei einem Datenverlust entstehen, bleibt damit fraglich. Versicherungsgesellschaften, die dieses Risiko abdecken, rechnen nach der Formel: 1 MByte Daten entspricht einem Wert von €000 (Quelle: TELA Versicherungs AG).

Dass eine solche Absicherung nicht ausreicht, kann leicht an zwei Beispielen errechnet werden:

1. Eine versierte Schreibkraft (durchschnittlich 300 Anschläge/min) kann Text mit einem Umfang von einem MByte optimal in ca. 55 Arbeitsstunden erfassen – vorausgesetzt, die Daten liegen als Ausdruck vor. Nimmt man einen Stundenlohn inkl. aller Nebenkosten von €40 an, dann kostet die ‚Datenwiederherstellung‘ auf diesem Weg ca. €200.
2. Ein Team aus drei Personen hat insgesamt 2,5 volle Arbeitstage an einer Kundenpräsentation gearbeitet; die Powerpoint-Präsentation ging bei einem Festplatten-crash verloren. Um die Präsentation aus den vorhandenen Brainstorming-Notizen und dem Recherchematerial zu rekonstruieren, braucht das Team noch einmal einen vollen Arbeitstag. Setzt man den Tag mit €600 pro Person an, kostete diese ‚Datenrettung‘ das Unternehmen €1.800.

Unternehmer zum Thema „Wert von Daten“

Rainer Maassen – Geschäftsführer bei *maassen & partner*, Hersteller von Datenbanklösungen:

„Der Wert von Daten hängt zunächst davon ab, inwieweit diese Daten unternehmenskritisch sind oder nicht. Davon hängt ab, wie weit ein vorübergehender Verlust der Daten bis zur Wiederherstellung Kosten verursacht. Außerdem spielt die Größe des Unternehmens eine Rolle. Die Daten eines Ein-Mann Betriebs können nicht so wertvoll sein wie die Daten eines Konzerns. Deshalb würde ich als Vergleichswert den Jahresumsatz nehmen.“

Kategorie 1: Alle Daten aus der Buchhaltung, Auftragsverwaltung und Lohnbuchhaltung sind besonders unternehmenskritisch. Ein Fehlen verursacht sofort erhebliche Kosten, mindestens in Höhe des Umsatzes, der in der Zeit vom Verlust bis zur Wiederherstellung gemacht würde und jetzt nicht gemacht werden kann. Dazu kommen Image-Nachteile usw. Mit anderen Worten: Die Daten sind unentbehrlich. Wenn sie gar nicht wiederhergestellt werden können, beträgt ihr Wert bis zu 50% des Unternehmenswertes, und der liegt üblicherweise beim 3- 5fachen des Jahresumsatzes.

Kategorie 2: Daten aus Vertrieb und Marketing, Kundendaten, Projektdaten usw. Deren Wert liegt bei 0,1 bis 0,5 Jahresumsätzen, je nachdem, wie wichtig die Daten für die Kundenbetreuung und die Außenkontakte sind.

Kategorie 3: Interne Daten, die nicht für die Leistungserbringung wesentlich sind. Aber auch ihre Kosten können erheblich sein.“

Unternehmer zum Thema „Wert von Daten“

Frank Brandenburg – Geschäftsführer Clearswift, Anbieter von Lösungen für die Sicherheit digitaler Kommunikation:

„Besonders als Softwareunternehmen wickelt man (fast) alles elektronisch ab. Ein gutes Beispiel dafür ist unsere Support-Datenbank. Wenn diese Daten nicht vorhanden wären, wüssten wir nicht:

1. welche unserer Kunden einen Support-Vertrag haben (und dafür auch bezahlt haben)
2. welche Produkte beim Kunden eingesetzt werden
3. welche Historie (Updates, bisherige Probleme) der Kunde hat

Diese Informationen liegen nur elektronisch vor, nicht zu sprechen von ‚banalen‘ Dingen wie Mailadressen, Telefon-Nummern etc.

Unser gesamtes Renewal- und Support-Geschäft käme damit zum Erliegen. Wenn man dabei gängige Umsatzgrößen bei Softwareherstellern betrachtet, beträgt der Supportanteil zwischen 30 - und 50%.

Diese Aussagen betreffen zunächst einmal Unternehmensdaten, die – wie allgemein üblich – auf einem Fileserver gespeichert und von dort aus auch gesichert werden.

Folgen von Datenverlust

Die Anzahl an Fällen von Datenverlust in Unternehmen und die Schwere der davon ausgelösten finanziellen Folgen nehmen seit Jahren massiv zu. Das liegt daran, dass

- immer mehr Unternehmen immer mehr Daten ausschließlich elektronisch speichern und keine Sicherung in Form von Ausdrucken mehr durchführen

Die Gesetzgeber in mehreren europäischen Ländern fördern diesen Trend: sie schreiben die Archivierung von Daten in Papierform nicht mehr für alle relevanten Wirtschaftsdaten zwingend vor, sondern akzeptieren die elektronische Archivierung. Entsprechende Gesetze sind bereits in Kraft getreten (z.B. in Deutschland) oder liegen zur Verabschiedung vor.

- Immer größere und technisch komplexere Speichersysteme eingesetzt werden, die – entgegen der landläufigen Annahme – insgesamt anfälliger für Datenverluste sind.

Die Speicherkapazität von Festplatten wurde in den letzten zehn Jahren um den Faktor 500 gesteigert. Das bedeutet: auf immer kleineren Flächen einer Platte befinden sich immer mehr Daten. Wird eine solche Platte mechanisch beschädigt, sind davon rund 500 mal mehr Daten betroffen als auf den Festplatten früherer Jahre!

- elektronische Daten immer lebenswichtiger für Unternehmen werden, da viele Geschäftsprozesse inzwischen zu hundert Prozent auf Daten und deren Verknüpfungen beruhen
- zwar immer bessere Backup-Systeme und -Methoden existieren, diese aber selbst in großen Unternehmen oft nicht konsequent oder nicht richtig eingesetzt werden

Kroll Ontrack-Recherchen haben ergeben, dass in 80% der Datenverlustfälle scheinbar ordnungsgemäß erstellte Backups existieren, dass sich aber herausstellt, dass sich die Backups in einem nicht verwertbaren Zustand befinden. Backup-Systeme gehen immer davon aus, dass die Hardware und die Speichermedien sich zum Zeitpunkt der Datensicherung in einem intakten Zustand befinden und die gesicherten Daten nicht beschädigt sind; lagen beim Mahen des Backups aber bereits Beschädigungen an Daten vor, dann wird das Backup dies einfach widerspiegeln. Die benötigten Daten können nicht wie gewünscht restauriert werden.

Man muss kein Schwarzseher sein, um die möglichen Folgen eines Datenverlustes für ein Unternehmen in düsteren Farben zu schildern:

- 93% der Unternehmen, deren Data Center für zehn oder mehr Tage ausfielen, überlebten das folgende Geschäftsjahr nicht (Quelle: National Archives and Records Administration U.S.A, Washington)

Datenverlust ist nicht einfach nur ein Schreckgespenst, mit dem Hersteller von Backup-Systemen ihren Umsatz steigern, sondern bittere Realität. Leider hilft auch das inzwischen übliche Sichern von Daten nicht immer. Können Daten tatsächlich einmal nicht von einem Backup restauriert werden, drohen einem Unternehmen massivste Folgen bis hin zum Konkurs.

Wie kommt es zu Datenverlust?

Im Gegensatz zu der in den Medien oft verbreiteten Meinung spielen Naturkatastrophen als Ursache für Datenverlust nur eine untergeordnete Rolle. Tatsächlich beruhen drei Viertel aller Schadensfälle auf Störungen an der Hardware oder auf Bedienungsfehlern.

Die fünf wichtigsten Ursachen für Datenverlust im Überblick

(Quelle: Kroll Ontrack-Studie, 2002)

- **Funktionsstörungen der Hardware oder des Systems -> 44%**

Mögliche Symptome:

- Fehlernachricht, die besagt, dass das Gerät nicht erkannt wird
- zuvor zugängliche Daten sind plötzlich nicht mehr auffindbar
- kratzende oder klappernde Geräusche
- Festplattenlaufwerk dreht sich nicht
- Festplattenlaufwerk des Computers arbeitet nicht

Gegenmaßnahmen:

- Schonen Sie elektrische Komponenten, indem Sie Ihren Computer vor Nässe, Licht und Staub schützen.
- Vermeiden Sie Spannungsschwankungen durch Verwendung einer unterbrechungsfreien Stromversorgung (USV)
- Schütteln Sie Festplattenlaufwerke oder Bänder nicht bzw. entfernen Sie die Abdeckungen nicht
- Stellen Sie sicher, dass Ihr Rechner – und damit auch die Festplatte – ausreichend Kühlung erhält. Überhitzungen können sowohl den Prozessor als auch die Festplatte schädigen.

- **Bedienungsfehler -> 32%**

Mögliche Symptome:

- Zuvor zugängliche Daten sind plötzlich nicht mehr auffindbar;
- Meldungen wie „Datei nicht gefunden“ werden angezeigt.

Gegenmaßnahmen:

- Führen Sie grundsätzlich keine Aktionen wie Installationen oder Reparaturen durch, mit denen Sie keine Erfahrung haben;
- vermeiden Sie es insbesondere, den Standort Ihres Computers während des Betriebs zu verändern.

- **Software-Fehler oder Funktionsstörungen von Software ->14%**

Mögliche Symptome:

- Systemnachrichten mit Bezug auf Speicherfehler
- Softwareanwendung lädt nicht
- Fehlermeldung, die besagt, dass Daten beschädigt oder unzugänglich sind

Gegenmaßnahmen:

- Sichern Sie regelmäßig Ihre Daten
- verwenden Sie Diagnose-Tools mit besonderer Vorsicht

- **Computerviren -> 7%**

Mögliche Symptome:

- Leerer Bildschirm
- seltsames und unvorhersehbares Verhalten
- Anzeige der Fehlermeldung „Datei nicht gefunden“, die einen Virenbefall andeutet

Gegenmaßnahmen:

- Arbeiten Sie mit einem guten Anti-Virus-Softwarepaket
- kaufen Sie Software nur bei seriösen Anbietern
- überprüfen Sie alle eingehenden Daten, einschließlich verpackter Software, auf Viren

- **Höhere Gewalt (Naturkatastrophen, Brände etc.) -> 3%**

Gefährdete Speichermedien

Grundsätzlich sind elektronisch gespeicherte Daten stärker gefährdet als Informationen, die auf Papier aufbewahrt werden. Zwar kann auch ein Aktenordner versehentlich weggeworfen werden oder einem Brand zum Opfer fallen – es gibt aber viel mehr mögliche Ursachen für den Verlust digitaler Daten. Hinzu kommt, dass digitale Informationen bis auf wenige Ausnahmen entweder in einem flüchtigen Speicher liegen, dessen Inhalt verloren geht, sobald die Stromzufuhr unterbrochen wird, oder auf Medien, die Daten magnetisch oder optisch aufzeichnen (Diskette, Festplatte, Magnetband, CD, DVD). Die Struktur solcher Medien kann durch eine Reihe von äußeren Einflüssen verändert werden (mechanisch, thermisch, magnetisch). Geschieht dies, so werden auch die gespeicherten Daten verändert. Wird z.B. durch den Magnetismus, den ein Lautsprecher abgibt, nur die geringe Anzahl von fünfzig Bytes einer Programmdatei auf einer Diskette verändert, kann dies dazu führen, dass diese Anwendung nicht mehr funktionsfähig ist.

Magnetisch und optisch gespeicherte Daten auf stationären Systemen

Die magnetische Speicherung von Daten hat eine lange Tradition, die bis zu den Kernspeichern von Großrechnern der 50er Jahre zurückreicht. Das Prinzip hat sich nicht wesentlich verändert: Jedes einzelne Bit (die kleinste digitale Informationseinheit, die jeweils den Wert 1 oder 0 darstellen kann) wird durch eine definierte Menge an Partikeln eines magnetisierbaren Materials dargestellt. Diese Menge ergibt sich aus der Fläche auf dem Datenträger, der wiederum als kleinste physikalische Speichereinheit definiert wird. Der Unterschied zwischen 1 und 0 wird durch die unterschiedliche Polung ausgedrückt.

Konkret: Ist die Mehrzahl der Partikel in einem Bereich in Nord-Süd-Richtung ausgerichtet, gilt dies als 0, ist sie in westöstlicher-Richtung gepolt, als 1.

Ausgerichtet werden die Partikel (heutzutage in der Regel aus Kristallen von Edelmetalloxiden bestehend) durch elektrische Spannung. In einer Festplatte ist dafür der Schreib-/Lesekopf zuständig, der in Mikrosekundengeschwindigkeit die Polung von Partikeln verändert. Gelesen werden solche Daten auf induktivem Weg: je nach der Polung wird im Schreib-/Lesekopf negative oder positive Spannung erzeugt, die dann als Wert 1 oder 0 interpretiert wird.

Während in früheren Jahren tatsächlich messbar große Bereiche von Platten mit Durchmessern von bis zu 12 Zoll (ca. 30 cm) für die Speicherung von einem Byte genutzt wurden, muss man bei aktuellen Festplatten meist schon in den molekularen Bereich schauen, um den Speicherbereich für ein Byte zu identifizieren. Ein übliches 2,5-Zoll-Harddisk-System mit 40 GByte Kapazität besteht z.B. aus drei einzelnen Leichtmetallplatten, die jeweils auf der Ober- und Unterseite beschrieben werden. Jede Oberfläche speichert also rund 2,5 GB. Das bedeutet, dass auf rund 400.000 mm² rund 2,7 Milliarden Bytes abgebildet werden! Die Datendichte liegt aktuell bei Werten oberhalb von 6.500 Bytes pro mm². Das veranschaulicht, wie verletzlich magnetisch gespeicherte Daten eigentlich sind.

Beeinflusst werden Magnetpartikel übrigens nicht nur durch magnetische Einwirkung. Der klassische ‚Headcrash‘, bei dem ein Schreib-/Lesekopf die Oberfläche berührt, führt zu einer physikalischen Beschädigung und damit zu Datenverlust. Hitze und Feuchtigkeit, die im Katastrophenfall einwirken, verändern meist die Struktur des Trägermaterials, so dass sich entweder die Magnetschicht teilweise ablöst oder aber der Träger (die ‚Platte‘) nicht mehr eben ist, was einen Headcrash zur Folge haben kann.

Die Daten eines Unternehmens werden heutzutage in der Regel zentral gelagert. Der so genannte ‚File Server‘ muss dabei aber nicht unbedingt ein Rechner mit einem Festplattensystem sein. Die Datenspeicherung kann durchaus auch verteilt stattfinden – z.B. auf mehreren Festplattensystemen an verschiedenen Orten oder in einem eigenen oder angemieteten Data Center. Zum Einsatz kommen dabei meist so genannte ‚Raid-Systeme‘, die aus einer beinahe beliebig ausbaubaren Anzahl einzelner Festplattensysteme bestehen und entsprechend große Datenmengen speichern können. Raid-Systeme oder auch Disk Arrays bestehen prinzipiell aus nichts anderem als einer Menge an softwaretechnisch verbundenen Festplatten. Der Unterschied zwischen mehreren in einem Rechner eingebauten Harddisks und einem Raid-System liegt nur darin, dass ein Raid-System mit einer eigenen Hard- und Software ausgestattet ist, die den Gesamtspeicher von außen als Einheit erscheinen lässt und durch automatisiertes Spiegeln von Daten für eine Redundanz der Informationen sorgt.

Für das Backup werden in den meisten Unternehmen nach wie vor Magnetbänder eingesetzt. Magnetbänder haben prinzipiell den Vorteil, dass für die Speicherung einer Informationseinheit mehr Fläche zur Verfügung steht, sodass die Daten magnetisch und mechanisch weniger gefährdet sind als auf einer Festplatte. Die Schreib-Lese-Methode unterscheidet sich nicht grundsätzlich, ist aber bei Magnetbändern insgesamt robuster. Trotzdem sind natürlich auch Magnetbänder – gleich welchen Typs: Streamerkassetten, Minikassetten, DAT etc.) – empfindlich gegenüber magnetischen, mechanischen und thermischen Einflüssen.

Als optische Medien werden – besonders im Bereich Datensicherung und mobile Daten – zunehmend auch CDs (als CD-ROM), DVDs oder magneto-optische Träger (MOs) eingesetzt. Diese sind zwar unempfindlich gegenüber externem Magnetismus, aber vor Datenverlust durch mechanische Beschädigung oder Hitze nicht gefeit.

Mobile Daten

Solange die Informationen zentral gelagert werden, lassen sie sich auch zentral schützen und kontrollieren. Doch wer schützt die Daten, die im Umlauf sind?

Mobile Geräte

Mobile Geräte beinhalten sensible Daten, z.B.:

- Notebooks, Laptops und Präsentationssysteme
- Pocket PCs, Palm Organizer, Psion Handheld Computer (EPOC) und andere PDAs
- Mobiltelefone, Diktiergeräte und Fotoapparate

Mobile Datenträger

Folgende mobile Speicher können sensible Daten enthalten:

- Disketten
- Magneto-Optische Platten (MOs)
- CD-Rs und CD-RWs
- DVD-Rs und DVD-RWs, DVD+Rs und DVD+RWs
- Streamerkassetten und Magnetbänder
- Wechselpplatten (Harddisk, ZIP, JAZ, u.a.)
- Compact-Flash-Speicher oder Microdrives
- Smart Medias
- Memory Sticks
- Secure Digital oder Multi Media Cards

Natürlich empfiehlt es sich zunächst, einfach Daten von mobilen Geräten und mobilen Datenträgern genauso zu sichern wie Daten von stationären Systemen. Im Idealfall wird die IT eines Unternehmens entsprechende Mechanismen und Richtlinien einsetzen, damit die Mitarbeiter dies auch tun können und müssen. So setzen sich langsam Lösungen durch, mit denen Außendienstmitarbeiter beispielsweise die Daten von ihrem Laptop über das Internet im Data Center des Unternehmens sichern können. Das Backup von Daten auf PDAs oder Mobiltelefonen bleibt aber in der Regel dem einzelnen Mitarbeiter überlassen, sodass die Datensicherheit hier vom individuellen Verhalten abhängt.

Speichermethoden

Grundsätzlich unterscheiden sich die Speichermethoden bei Platten und Bändern voneinander. Während bei Platten (einschließlich CD-ROMs, DVDs und MO) die Daten wahlfrei geschrieben und gelesen werden können, sind sie auf Bändern sequenziell gespeichert. Das bedeutet, dass einzelne Datenbereiche bzw. ganze Dateien auf einem Band nur durch Vor- und Rücklauf angesteuert werden können. Bei einer Festplatte sorgt das jeweilige Betriebssystem dafür, dass der physikalische Aufbewahrungsort eines Datenpartikels in Tabellen abgelegt wird. Diese Information wird dann zur Ansteuerung der gewünschten Information genutzt.

Bei einer ‚klassischen‘ Festplatte ist das Betriebssystem dafür verantwortlich, eine solche Tabelle (in der DOS-/Windows-Welt File Allocation Table = FAT genannt) zu erzeugen und zu verwalten. Was PC-Anwender möglicherweise als ‚Formatieren‘ kennen, ist eigentlich der Vorgang, bei dem eine solche Tabelle angelegt wird. Vereinfacht dargestellt kann man sagen, dass sie zunächst dem jeweils kleinstmöglichen Aufbewahrungsort für ein kleinstmöglich abbildbares Datenstück (in der Regel: ein Byte) eine feste Adresse zuschreibt. In den meisten Fällen wird die Oberfläche der Platte dazu in Spuren eingeteilt, die aus konzentrischen Kreisen definierter Breite bestehen. Die zweite Dimension bilden die so genannten ‚Sektoren‘, die man sich vorstellen kann wie Stücke einer Torte. Auf diese Weise kann anschließend beispielsweise der Sektor 112 auf Spur 18 angesteuert werden.

Die kleinsten adressierbaren Einheiten dieser FAT Dateizuordnungstabelle sind die Cluster. Ein Cluster fasst mehrere **Sektoren** zusammen. Die Anzahl hängt dabei von der **Partitionsgröße** und dem **Dateisystem** ab.

Bei einer FAT16 Partition können maximal 0xFFFF hex Cluster adressiert werden. Dies ist gleichbedeutend mit 65535 Einträgen in der FAT oder auch 65535 Clustern, die benannt werden können!

Folgende Tabelle veranschaulicht die Berechnung:

Partition Size MB	Sectors per Cluster	Bytes per Cluster
16 – 127	4	2048
128 – 255	8	4096
256 – 511	16	8192
512 – 1023	32	16384
1024 – 2047	64	32768

Die maximale Größe einer Partition berechnet sich dabei wie folgt:

max. Anzahl der FAT Einträge * Sectors per Cluster * 512 Byte/Sector. Bei Clustergröße 8 ergeben sich demnach maximal $65535 * 8 * 512 = 268431360$ bytes, also 262140 kbyte oder 255 MB. Für eine FAT32 Partition gilt: Maximal 0x0FFF FFFF = 268 435 455 Cluster können adressiert werden, bei Clustergröße 8 sind dies demzufolge 1 023,9 GB, also über ein Tera Byte!

Diese Darstellung gilt in dieser Form natürlich nur für FAT-Dateisysteme. Festplatten, die mit einem anderen Dateisystem, beispielsweise dem aus der UNIX-Welt bekannten NTFS, arbeiten, können hier andere Ordnungsstrukturen aufweisen.

Betrachten wir wieder das populäre FAT-Dateisystem, das den meisten Anwendern aus dem täglichen Umgang mit der Windows-Welt vertraut ist. Wird hier eine Datei gespeichert, sucht das Betriebssystem nach einem freien - genauer: freigegebenen Cluster und schreibt die Bytes der Datei dort hinein. Wird eine Datei gelöscht, gibt das Betriebssystem diesen Sektor wieder frei – aber: die physikalische Datenspeicherung, also die Polung der Magnetpartikel wird dabei nicht verändert! Da ein Cluster idealtypisch (dies variiert von Betriebssystem zu Betriebssystem und von Harddisk-System zu Harddisk-System) 512 Byte speichert und eine Datei in der Regel aus Tausenden von Bytes (= KByte) besteht, müssen mehrere Cluster beschrieben werden. Da oft nicht der physikalisch nächstliegende Sektor frei ist, muss ein Ort für die Folge-Bytes gesucht werden. Deshalb verzeichnet die Dateitabelle nicht nur, welche Cluster frei(gegeben) sind und in welchen Clustern welche Bytes liegen, sondern auch, in welchem Cluster eine Datei beginnt und wo sie weitergeht. So entsteht eine Kette aus Clustern, die aufeinander verweisen und nacheinander ausgelesen die Datei ergeben, die benutzt werden soll.

Diese grundsätzliche Methode hat aber auch Nachteile. Da in Wirklichkeit eine Datei nicht nur einen Cluster umfasst, sondern um ein Vielfaches größer ist, kann es sein, dass der letzte Rest einer Datei einen Cluster nicht ausfüllt. Es bleibt Platz (der so genannte ‚Slack‘) übrig, der eventuell noch physikalisch Daten enthält, die jedoch im Dateisystem nicht mehr zugeordnet werden, da sie zu keiner aktuell genutzten Datei gehören.

Diese „versteckten“ Restdaten und der Umstand, dass beim Löschen von Dateien die Daten nicht wirklich entfernt werden, sondern nur aus dem „Inhaltsverzeichnis“ der Festplatte gelöscht werden, damit der benutzte Speicherplatz überschrieben werden kann, bieten der Datenrettung große Chancen. Denn: Physikalisch vorhandene Daten, also solche, die in Form unterschiedlicher Polung von Magnetpartikeln existieren, können wiederhergestellt werden. Das gilt genauso auch für Daten auf Magnetbändern und ähnlich für optisch gespeicherte Daten.

Diese „versteckten“ Restdaten und der Umstand, dass beim Löschen von Dateien die Daten nicht wirklich entfernt werden, sondern nur aus dem „Inhaltsverzeichnis“ der Festplatte gelöscht werden, damit der benutzte Speicherplatz überschrieben werden kann, bieten der Datenrettung große Chancen. Denn: Physikalisch vorhandene Daten, also solche, die in Form unterschiedlicher Polung von Magnetpartikeln existieren, können wiederhergestellt werden. Das gilt genauso auch für Daten auf Magnetbändern und ähnlich für optisch gespeicherte Daten.

Methoden der Datenrettung

Eines bleibt festzuhalten: Die einzige und beste Prophylaxe gegen Datenverlust ist ein konsequent durchgeführtes Backup! Aber selbst wenn diese Vorbeugungsmaßnahme in einem Unternehmen optimal verwirklicht wird, bleibt ein Restrisiko. Mit den modernen Methoden der Datenrettung lassen sich jedoch auch Daten, die nicht aus einem Backup restauriert werden können, wiederherstellen.

Die Aufgaben der Datenrettung liegen nicht nur in der aufwändigen Wiederherstellung von Datenfragmenten auf beschädigten Datenträgern. Neben dem komplexen Finden und Auslesen von Magnetpartikeln und „Datensplittern“ gibt es zahlreiche Fälle, bei denen es ausreicht, redundante Daten auf gespiegelten Systemen zu identifizieren oder aus dezentral gesicherten Informationen zusammensetzen. Mit der genauen Kenntnis des Betriebssystems, der vorhandenen Netzstruktur und der für diesen Fall geeigneten Werkzeuge zur Datenrettung kann durch einen professionellen Eingriff oft eine rasche und erfolgreiche Datenrecherche eingeleitet werden.

Wiederherstellung der Daten

Aufgrund genauer Systemkenntnisse wissen die Experten, welche Daten in welchen Verzeichnissen, Sektoren oder Segmenten von Datenträgern zu finden sind und was eine rasche und effiziente Wiederherstellung gelöschter Dateien möglich macht. Gelöschte Daten lassen sich relativ leicht wiederherstellen, sofern mit dem entsprechenden Rechner nicht allzu lange weiter gearbeitet wurde und somit Daten überschrieben wurden. Darüber hinaus lassen sich Datei-Fragmente in freigegebenen Clustern und im Slack-Bereich (von Dateien nicht ausgenutzte Bereiche) der Festplatte auffinden.

Selbst von formatierten Festplatten und beschädigten Datenträgern lassen sich Daten gezielt wiederherstellen, wobei auch zunächst nicht mehr lesbare, korrupte Dateistrukturen kein dauerhaftes Hindernis bieten. Selbst wenn sich durch physische Zerstörungen – beispielsweise fehlende Stücke des Magnetbandes – nur Teile des Datenträgers wiederherstellen lassen, kann dies durchaus genügen, da dieser Teil eventuell wichtige Informationen, den verlangten Nachweis oder das fehlende Indiz enthält.

Viele verloren geglaubte Informationen lassen sich zudem aus gelöschten E-Mails oder über die Wiederherstellung von Meta-Daten retten. Hier wird deutlich, wie wichtig die genaue Kenntnis von Betriebssystemen und deren Eigenheiten ist

Daher ist es von großer Bedeutung, dass der Experte genau weiß, wie Dateien, die Lücken haben, aufgefüllt werden können, so dass sie logisch als vollständige Dateien erkannt werden. Korrupte Dateien werden über Software-Werkzeuge lesbar gemacht, so dass alles, was außerhalb des korrupten Bereiches liegt, wieder gelesen werden kann. So lassen sich auch Dokumente, deren Header beschädigt sind, restaurieren und wieder öffnen, was bei korrupten Dateien sonst vom Betriebssystem verweigert wird.

In rund 60 Prozent aller Fälle sind die Daten so schwer beschädigt, dass die Festplatte in den Reinraum muss. In einem hochspezialisierten Prozess werden hier verlorene Daten gesucht und wiederhergestellt, Verzweigungen und Strukturen rekonstruiert und die Daten auf neuen Medien sicher abgespeichert.

Datenrettung im Labor / Reinraum

Wenn absehbar ist, dass System- und Strukturanalyse auf dem Weg zu den gesuchten Daten nicht weiterkommen, ist es Zeit für den Reinraum-Ingenieur, seinen weißen Kittel überzustreifen und sich mit Feinmechanik und Fachwissen auf die Spur des Datenbestandes zu machen. Hier ist dann die perfekte Zusammenarbeit zwischen Analytiker und Mechaniker gefragt, denn von außen betrachtet sind alle Daten gleich. Nur in einer perfekten Suche nach vorgegebenen Mustern in den logisch als relevant erachteten Sektoren lässt sich zielgerichtet vorgehen. Anders ist eine Recherche auf gigabyte-großen, gelöschten und oft stark beschädigten Datenträgern kaum effizient durchführbar.

Der erste Schritt bei der Datenrettung im Labor ist immer der Versuch, alles, was physikalisch auf dem beschädigten Datenträger gespeichert ist, auf ein intaktes Speichersystem zu übertragen. Im einfachsten Fall bedeutet dies, mit einem geeigneten Softwaretool die Daten eins-zu-eins auf eine neue Festplatte gleichen Typs zu übertragen, so dass ein physikalisch vollständig identisches Abbild entsteht. Grundsätzlich nehmen Datenrettungsexperten ihre Wiederherstellungsversuche nicht am Original-medium vor, da jeder Versuch den Verlust weiterer Daten zur Folge haben könnte.

Schwieriger wird es, wenn ein Harddisk-System mechanisch so beschädigt ist, dass sich die Platten nicht mehr drehen oder die Schreib-/Leseköpfe defekt sind. Dann muss das Gerät im Reinraum geöffnet werden. In einem solchen Reinraum – wie bei Kroll Ontrack in Böblingen – herrschen ähnliche Bedingungen wie an den Produktionsstätten der Festplatten. Hier wird dafür gesorgt, dass sich Staubpartikel nicht auf der empfindlichen Plattenoberfläche ablagern können und eine zu hohe Luft-feuchtigkeit nicht zu Kondenswasser auf dem Material führt. Beides würde in jedem Fall zu weiterem Datenverlust führen. Oft werden beschädigte Systeme komplett demontiert, die einzelnen Platten entnommen und in einem neuen Gehäuse mit neuen Schreib-/Leseköpfen und einer neuen Platine wieder zusammengesetzt. In nicht wenigen Fällen können von einer derart mechanisch rekonstruierten Festplatte alle Daten vollständig und ohne Fehler auf ein neues Harddisk-System übertragen werden.

Dieses Verfahren betrifft nur Datenträger, die durch ‚höhere Gewalt‘ nach einem Brand- oder Wasserschaden oder durch mechanische Überbeanspruchung (Sturz aus großer Höhe, massive Erschütterung im laufenden Betrieb etc.) beschädigt wurden. Bei Wasserschäden geht der mechanischen Bearbeitung übrigens ein Trocknungsverfahren voraus, wie es aus der ‚klassischen‘ Schadensanierung bekannt ist. Nach Brandschäden müssen in der Regel Platten und Köpfe unter Einsatz von Feinmechanik unter dem Mikroskop voneinander getrennt werden. Genauso aufwändig stellt sich die Datenrettung dar, wenn die logische Anordnung der Daten durch Software- oder Bedienungsfehler bzw. Viren in Unordnung geraten ist. Hier muss wiederum der gesamte Inhalt der Festplatte Byte für Byte ausgelesen und übertragen werden.

Je nach Beschädigung kann ein solcher Lesevorgang durchaus einige Stunden, aber in Ausnahmefällen auch mehrere Tage oder Wochen dauern - eine Spanne, die für den Auftraggeber nicht nur sehr teuer, sondern bei zeitkritischen Daten auch deutlich zu lange ausfallen kann. Hier lässt sich mit der genauen Kenntnis des Installations-verhaltens von Betriebssystemen und Programmen, der automatischen Verwaltung von temporären und Auslagerungsdateien und der Vorgehensweise von Tools wie beispielsweise Festplattenoptimierern der Vorgang deutlich beschleunigen.

Die Schritte bei der Datenrettung im Labor:

- Wenden Sie sich an ein Datenrettungsunternehmen, z.B. Kroll Ontrack
0800 10 12 13 14 (D), 0800 644 150 (A), 0800 880 100 (CH)
- Verpacken Sie das betroffene Speichermedium entsprechend der Anweisungen und schicken Sie es an das Labor des Datenretters.
- Der Datenrettungsspezialist führt eine Diagnose durch und informiert Sie über das Ergebnis.
- Nach der Auftragserteilung durch Sie wird die Datenrettung vorgenommen.
- Die rekonstruierten Daten werden auf CD/DVD, Magnetband o.ä. gesichert.
- Die Daten werden Ihnen zugeschickt, und Sie können diese wieder in Ihr System einspielen.

Tatsächlich ist es so, dass Defragmentierer bei der Datenwiederherstellung unerwartete Schwierigkeiten bereiten können, da beim so genannten „Aufräumen“ der Platte alte „Slack“-Datei überschrieben werden können. Keinerlei Chance zur Wiederherstellung von Daten gibt es, wenn ein spezielles Tool zum Löschen von Daten eingesetzt wurde, das die leeren Bereiche der Festplatte mit Datenmustern überschreibt. Was unter dem Aspekt der Datensicherheit durchaus wünschenswert ist, kann bei der Suche nach verlorenen Daten älteren Datums die Recherche deutlich erschweren. Anwender sollten ebenso wie Systemadministratoren darauf achten, dass ihre PCs so wenig „Eigenleben“ wie möglich führen. Einerseits liegt hier oft die Quelle für spätere Probleme, andererseits können solche Eigeninitiativen auch unabsichtlich Angriffe von innen und außen verdecken. Wer sich einmal daran gewöhnt hat, dass seine Festplatte durch die Hintergrundaktivität eines Utilities anläuft und Daten transferiert, wird auch nicht aufschrecken, wenn die gleiche Aktion von einem Trojaner oder einem anderen Angreifer ausgelöst wird. Je besser ein Anwender sein System kennt, je genauer er die Programme im Blick hat, die ihn bei der Arbeit unterstützen und je konsequenter er sich auf diese umgrenzte Palette beschränkt, umso sicherer ist sein Rechner und umso sensibler und schneller kann er auf ungewohnte Aktionen reagieren - im Krisenfall gar durch entschlossenes Ziehen des Netzsteckers.

Online-Datenrettung

Noch recht jung am Markt aber schon überaus erfolgreich ist die Online-Datenrettung, wie sie derzeit von Kroll Ontrack als einzigem Datenrettungsunternehmen unter dem Namen Remote Data Recovery (RDR®) angeboten wird. Die Entwicklung dieser Methodik beruht auf der Erfahrung, dass in ca. 50% der Fälle das Einschicken eines Datenträgers nicht nötig gewesen wäre, da der Datenverlust nicht aufgrund einer Beschädigung des Speichermediums entstanden ist, sondern durch korrupte Dateisysteme, Fehlbedienung oder Viren ausgelöst wurde.

Solche Fälle von Datenverlust können auch ohne Analyse der betroffenen Hardware gelöst werden. Für die Kunden hat dies erhebliche Vorteile, insbesondere, was den Zeitaufwand für die Datenrettung angeht. Schließlich muss bei einer Datenrettung im Labor – abgesehen von der Zeit für Einsenden und Zurückschicken der Medien – oft mit drei bis fünf Tagen gerechnet werden. RDR® steht dagegen 24 Stunden am Tag zur Verfügung und ist die derzeit schnellste Form der Datenrettung. Die Kontaktaufnahme mit dem Datenretter erfolgt per Telefon, die Datenanalyse per Software im telefonischen Kontakt mit dem Experten, der dann die möglicherweise nötige Datenrekonstruktion online vornimmt.

Möglich ist die Online-Datenrettung derzeit für folgende Betriebssysteme:

- DOS
- Windows 3.x, 95, 98, Me, 2000, NT und XP
- Linux
- Novell NetWare

sowie für

- Microsoft SQL
- Microsoft Exchange Server

Grundsätzlich möglich ist die Online-Datenrettung immer dann, wenn ein Laufwerk physikalisch gesund ist. Dann können die Daten auf diesem Laufwerk über eine gesicherte Modem- oder Internetverbindung direkt bearbeitet und wiederhergestellt werden. Dabei ist es egal, ob es sich um einen Server, Desktop oder Laptop handelt. Kroll Ontrack setzt ein eigenes (geheimes) Übertragungsprotokoll ein, das durch eine Datenverschlüsselung auf Paketbasis zusätzlich optimiert wird.

Und so läuft eine Remote-Datenrettung ab:

- Sie stellen eine Verbindung zu einem der RDR-Server her; dazu benutzen Sie den speziellen Client, der Ihnen mit dem RDR-QuickStart-Paket zur Verfügung gestellt wird. Diese Software können Sie in der zu Ihrem Betriebssystem passenden Version bekommen. Für den Fall, dass Ihr System nicht mehr hochfährt sogar auf einem bootfähigen Datenträger.
- Über diese Verbindung treten Sie in Kontakt mit einem der Kroll Ontrack-Ingenieure.
- Dieser RDR-Ingenieur kann mit einer speziell entwickelten Software eine Analyse Ihrer Daten durchführen; zuvor wird ein Tool installiert, das alle Veränderungen an den Daten aufzeichnet und veränderte Daten sichert, so dass Ihr System im Zweifelsfall komplett in den Ausgangszustand versetzt werden kann. Die Analyse durchläuft üblicherweise die folgenden Schritte:
 - Test auf physische Integrität des betroffenen Systems;
 - Einschalten des Track-/Backup-Tools;
 - Remote-Tools ermitteln die Ursache des Datenverlusts;
 - Ermittelte Probleme werden behoben und Veränderungen geschrieben;
 - der RDR-Ingenieur beendet die Verbindung, Sie booten das System neu;
 - Sie haben wieder Zugriff auf Ihre Daten!

Ziel der RDR ist es, dass der Rechner wieder booten kann und Zugriff auf die Daten wieder besteht.

Praktische Anwendungsfälle für die Online-Datenrettung

Wie gesagt: Logische Problemfälle können fast immer mit der Remote Data Recovery gelöst werden. Es gibt sehr oft eine Reihe typischer Situationen, in denen dieses Verfahren die schnellste und kostengünstigste Variante darstellt.

Wiederherstellung von RAID-Systemen

Wenn die Störung an einem RAID-System dazu führt, dass dieses vom Fileserver-Betriebssystem nicht mehr erkannt wird, stehen die gespeicherten Daten nicht mehr zur Verfügung. Bisher war die einzige Lösung, den RAID-Server neu aufzusetzen und die Daten von Backup-Bändern zu restaurieren. Im Extremfall führt dies zu einem mehrtägigen Systemausfall.

Kroll Ontrack RDR hilft auch hier, da sich der RDR-Ingenieur auch in den RAID-Server einklinken, dort die Diagnose und schließlich die Datenrettung durchführen kann. In der Regel ist dies eine Sache von wenigen Stunden.

Wiederherstellung von MS Exchange Servern

Der Ausfall eines Mailservers ist für viele Unternehmen einer der schlimmstmöglichen Unfälle, da oft stunden-, wenn nicht tagelang keine E-Mails und Faxe empfangen und versendet werden können und so die Kommunikation mit Kunden und Partnern praktisch zum Erliegen kommt. Da sich die Daten auf einem solchen Mailserver durch ein- und ausgehende Mails und Faxe im Sekundentakt ändern, hilft ein Restore von Sicherungsbändern, die in der Regel einmal täglich erzeugt werden, meist nicht weiter. Bei einem MS Exchange Server kann es zu Inkonsistenzen in der Datenbank kommen, wenn z.B. kurzzeitig die Stromversorgung ausfällt.

In diesem Fall kann der RDR-Ingenieur die Datenbankstruktur per Remote-Zugriff

analysieren, die einzelnen Mailboxen der Anwender als PST-Dateien extrahieren und dem Kunden zur Verfügung stellen. Diese PST-Dateien zu importieren und daraus eine neue Exchange-Datenbank aufzubauen, ist dann für den Systemverwalter nur noch eine Routinetätigkeit.

Wiederherstellung von MS SQL Servern

Ganz ähnlich kann auch der Ausfall eines Datenbank-Servers vom Typ Microsoft SQL behoben werden. Auch hier analysiert der RDR-Ingenieur zunächst die Struktur, sucht intakte Datensätze und überführt diese in eine intakte Datenbank. Diese enthält dann alle Datensätze bis auf die beschädigten.

Wiederherstellung nach einem Virusangriff

Der Schlüssel zum Erfolg der Online-Datenrettung RDR nach einem Virenangriff ist die RDR-QuickStart-Software. Mit der bootfähigen Version kann das betroffene System neu gestartet werden, ohne dass die Gefahr besteht, dass der Virus weiteren Schaden anrichtet. Der RDR-Ingenieur kann sich auf dem befallenen System einloggen, den Virus entfernen und beschädigte Daten rekonstruieren.

Wiederherstellung versehentlich gelöschter Daten

Wer hat noch nie versehentlich wichtige Dateien gelöscht? Meist passiert das unterwegs auf dem Notebook – weit ab von jeder Hilfe durch den IT-Administrator des Unternehmens. Auch hier kann eine RDR helfen, da man als Betroffener von jedem Ort der Erde aus mit einem RDR-Ingenieur in Verbindung treten kann, der den Schaden behebt und die gelöschte Datei online wiederbelebt.

Datenrettung mit Software-Tools

Es gibt nur wenige Fälle von Datenverlust, in denen Sie als Anwender selbst verloren gegangene Daten wiederherstellen können – und auch nur dann, wenn Sie ein erfahrener Anwender oder IT-Profi sind und dementsprechend Profi-Tools einsetzen. Leider wird gerade für den Einzelplatz-PC eine Reihe von Software-Produkten angeboten, die im Zweifelsfall den Schaden nur noch vergrößern. Allein schon die Tatsache, dass einige Tools zwingend verlangen, auf dem betroffenen System installiert zu werden, zeigt die potenzielle Gefahr. Schließlich gilt: Jeder Schreibvorgang auf einem Speichermedium, auf dem Daten verloren gegangen sind, verringert die Chance zur Datenrettung!

Do-it-yourself-Datenrettung ist daher überhaupt nur in folgenden Fällen angeraten:

- Versehentliches Löschen von Daten
- Wiederherstellen von Daten nach Virenbefall
- Nichtzugreifbare Daten aufgrund von Partitionierungsproblemen

Die simpelste Form von Datenrettungs-Software ist in der Lage, versehentlich gelöschte Dateien auf einem DOS- oder Windows-PC wiederherzustellen, so lange kein Schreibvorgang nach dem Datenverlust durchgeführt wurde. Allerdings ist es nur dann ratsam, solche Tools einzusetzen, wenn ganz sicher ist, dass die verschwundenen Dateien tatsächlich versehentlich gelöscht wurden und nicht durch andere Ursachen verloren gegangen sind.

Die Möglichkeit, Daten wiederherzustellen, die bei einem Virenangriff zerstört wurden, ist Bestandteil von guter Anti-Viren-Software. Vorsicht! Werden in diesem Fall Tools zum Wiederherstellen versehentlich gelöschter Dateien eingesetzt, können sie den Schaden vergrößern.

Datenrettungsunternehmen wie Kroll Ontrack setzen inzwischen auf eine Mischung von Do-it-yourself-Verfahren und Datenrettungs-Services. Mit dem Softwarepaket Easy Recovery Professional stehen IT-Profis einige der Tools zur Verfügung, die auch bei der professionellen Datenrettung zum Einsatz kommen. Erreicht der Kunde aber mit dem Einsatz dieser Tools nicht sein Ziel, kann er telefonische Beratung und Unterstützung bei der Datenrettung in Anspruch nehmen.

Kroll Ontrack GmbH
Hauptsitz Böblingen
Hanns-Klemm-Str. 5
71034 Böblingen
Fon +49 (0)7031 644-0
Fax +49 (0)7031 644-100
Datenrettungs-Hotline:
0800 10 12 13 14

info@krollontrack.de
www.ontrackdatarecovery.de

Kroll Ontrack S.a.g.l.
Piazza Boffalora, 4
P.O. Box 191
6830 Chiasso 3 Boffalora
Fon +41 (0)91 68286-92
Fax +41 (0)91 68286-94
Datenrettungs-Hotline:
0800 880 100

info@krollontrack.ch
www.ontrackdatarecovery.ch

Kroll Ontrack GmbH
Zweigniederlassung Österreich
Landstraßer Hauptstraße 71/2
1030 Wien
Fon +43 (0)1 71728-380
Fax +43 (0)1 71728-110
Datenrettungs-Hotline:
0800 644 150

office@krollontrack.at
www.ontrackdatarecovery.at

Copyright © 2008 Kroll Ontrack Inc.
All Rights Reserved.

All other brands and product names are
trademarks or registered trademarks of

KROLL ONTRACK®

Vertrauen Sie auf die Besten.